View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2009 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2009

Bio-Nanotechology: A Human Attack Vector

Sue Conger
University of Dallas

Follow this and additional works at: http://aisel.aisnet.org/confirm2009

Recommended Citation
Conger, Sue, "Bio-Nanotechology: A Human Attack Vector" (2009). *CONF-IRM 2009 Proceedings*. 18.
http://aisel.aisnet.org/confirm2009/18

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CONF-IRM 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

9. BIO-NANOTECHOLOGY: A HUMAN ATTACK VECTOR

Sue Conger,
University of Dallas, USA

Abstract

At present, humans could be direct targets of hacked bio- or nanotechnologies. This paper describes the future of biotechnology and nanotechnology, focusing on smart motes and bio-engineered products based on genome mapping. Then threats from these emerging technologies are developed to show different attack potentials. Finally, alternative development activities are proposed that mitigate the risks posed to humans.

Keywords:

Nanotechnology, Biotechnology, Emerging Technology, Risk

1.Introduction

In March 2008, an Internet attacker posted hundreds of messages laced with flashing graphics to the Epilepsy Foundation web site that caused patrons of the web symptoms ranging from headaches to seizures (EpilepsyFoundation.com, 2008). This attack, while not using nanotechnology, represents a turning point in Internet attacks where the intended target and harm is not a computer, but a human being. With this attack in mind, embedded bionanotechnology that is ingested or implanted spawns the same concern: Could embedded bionanotechnology be an attack vector to a person?

In the near future, foods and drinks will be laced with smart nano-sized devices to maintain product authenticity and tamper resistance. However, there is no consumer means to strip these devices out of a bottle of water or steak. Thus, consumers will have these devices in them for an unknown amount of time. The concern is that these agents could be compromised or otherwise hacked before they are ingested. Once inside the body, the human immune system would be unaware or neutralized to their presence, awaiting a command or trigger. The trigger could be the presence of another embedded bionanotechnology or could be an external stimulus from radio, light, or sound. Such a scenario could pose a threat to human viability.

From Richard Feynman's 1959 speech "There's Plenty of Room at the Bottom," science has focused on ever-smaller and more intelligent agents to perform routine tasks. The field of nanotechnology has discovered that scientific laws 'in the large' do not apply 'in the small.' Buckyballs, a new form of carbon developed as part of this small science, have properties that are unique: One cell thick 'walls' that comprise carbon nanotubes (CNTs) are the strongest creations in nature, can be conductive of electricity and/or fluids, can change characteristics, and are the basis of much of the new science.

Similarly, in the biotechnology realm, genetic engineering made possible by genome mapping has revolutionized food production and is beginning to be applied to almost every manufacturing area.

Combining biotechnology and nanotechnology will allow smart, reprogrammable, self-replicating organisms that are self-organizing networks of independent actors that can be programmed to perform just about any task. As Angela Belcher of MIT says, "Bacteria are just a factory to make viruses, and the viruses are just a tool to build electrodes ." The benefits of such technological revolutions seems obvious. Less obvious are the risks to human life posed by the technologies. This paper explores the characteristics of biotechnology and nanotechnology to describe the technology and to develop a list of risks posed to human health. Then, several proposals are made to prevent the risks identified.

2.Biotechnology and Nanotechnology

2.1.Biotechnology

Biotechnology applies biological processes, organisms, or systems in the development of products intended to improve the quantity and quality of life (whatis.techtarget.com; Anton, et al 2001). Biotechnology has literally millions of applications ranging from medicine to industry to marine life to the environment. Problems that perplex us today will eventually be mitigated through some form of bioengineering.

The basis of biotechnology is the cell. Each cell in every living organism contains a complete set of deoxyribonucleic acid (DNA), which dictates the organism's traits and behavioral characteristics (US DOE, 2008). Genome is the term for an organism's DNA. Genomes range from 600,000 to three billion base DNA pairs. In humans, DNA is expressed in 46 chromosomes, each with a separate DNA molecule that ranges from 50 million to 250 million base pairs. "The human genome contains 3.2 billion chemical nucleotide base pairs (A,C,T, and G) … [with] millions of locations where single-base DNA differences occur in humans" (US DOE, 2008, pg 3).

Chromosomes contain genes, which determine inherited traits. "The human genome is estimated to contain some 25,000 genes" US DOE, 2008, p 1). Proteins are macromolecules in cells that are comprised of three-dimensional strands of amino acids responsible for most cellular life functions (US DOE, 2008; Wikipedia, 2008). The study of proteins, proteomics, seeks to understand the basis for disease by analyzing the continuously changing chemical responses that are the protein-level responses to changing physical contexts. The sheer numeric complexity of genomic and proteomic variation is beginning to yield broad results. One map for genes and proteins contains five different characteristics for each: Structure, expression, variation, function and integration (CHIDB.com, 2008). Each unique combination of characteristics much be understood and controlled in the creation of biotechnology products.

Eventually, every disease from acid reflux to yellow fever can and will be treated by biotechnology means. Research covers over 100 delivery methods and many thousands of diseases. Some issues are separating truth from fiction in the research conducted. Many studies

have brought initial euphoria and hope only to be found unreplicable and not delivering the results promised (cf. Science; Nature; Lancet; PNAS, and other medical and scientific journals).

Another hindrance to progress in biotechnology is complexity. First is the problem of numeric complexity; second is the problem of cognitive and scientific complexity. There are over 400,000 organizations working in the biosciences. Managing the flood of data to develop globally accepted and accessible ontologies and taxonomies has proven difficult. For instance, when a global organization was slow in agreeing on an ontology for one area of biotechnology, a small group of countries developed and used their own ontology, inviting the global group to adopt their definitions. Unfortunately, the global group went its own way and thus, there are multiple non-reconcilable, and not easily integratable, sets of research information. Rather than helping get information out earlier, the group that uses their own methods of classification have created another 'language' that must be translated to be useful.

The second issue of cognitive complexity of biosciences is also daunting. Concerted projects such as the bio-grid projects seek to focus energies on specific problems, thereby speeding solutions. However, even with a profit motive, the path to bringing complex products to market can be 16 years or ore (Bio.org, 2006).

Another aspect of cognitive complexity is the need for ever more complex technology to support the search for similarities and differences between genes and proteins. New automation and materials sciences have been developed to support analysis at the atomic level. Significant program code is required to run the new equipment. These tend to be subject to significantly more sophisticated and exact specification and quality control than any business programs, but they are still error-prone.

A whole new field of bioinformatics have developed to manage and analyze the complex data generated from genomics and proteomics studies. Bioinformatics combines disciplines from computer science and data base technology with mathematics and statistics to the study of macromolecular structures, genome sequences, and the results of functional genomics experiments (e.g. expression data) (Luscombe, et al., 2001). The ACTION-Grid project funded by the European Union is a project to design and implement large-scale computing and knowledge management support for bio-medical informatics, nano-technology, and grid computing technology, using service-oriented architecture approach for the software (Action-Grid.EU, 2008). Use of novel technologies always is fraught with the same movements forward and back as errors force rethinking and new techniques are needed. Thus, the technology aspects of Action-Grid, once successful, should provide global resources to improve knowledge management in and across organizations.

2.2. Nanotechnology

Nanotechnology is based on the science of the small, defined as work performed at the molecular level (PCMag.com, 2008). 'Nano' means one-billionth (10^9), thus, work in nano-meters is work at the one-billionth of a meter level (e.g., 80,000 times smaller than the width of human hair). Nanotech devices can have as few as 15 molecules which each perform some unique function with one computing device, one communicating device, and one or more action devices in a unit.

One common form of not-quite-nano-technology is "Micro-Electro-Mechanical Systems (MEMS), which is the integration of mechanical elements, sensors, actuators, and electronics on a common silicon substrate that measure … mechanical, thermal, biological, chemical, optical, and magnetic phenomena" (Memsnet.org, 2008, pg 1). MEMS, microscopic sized devices, and nanotechnology are often discussed together because MEMS are used in many devices that work on a nano-scale, such as scanning tunneling microscopes. Initial MEMS were simply small mechanical devices, but integrating circuits along with sensors on the same silicon enables intelligence through programming. MEMS devices are replacing other, large, non-integrated, more costly technologies such as accelerometers in air bag deployment systems (Memsnet.org, 2008).

The nanotechnology level of work is even more like science fiction. Nanotechnology science has developed machines that build other machines. The machines build atomically precise structures consisting of specific arrangements of atoms. These functional nanostructures process either energy, some material, or information (Foresight.org, 2007).

At the molecular level, science in the large does not apply. For instance, laws of gravity and inertia disappear at the atomic level (Memx.com, 2008). This has caused the development of whole new sciences of physics, chemistry, and materials manufacturing to define atomic operations.

Computing at the molecular level requires a 'Tiny OS®' or other operating system with a limited instruction set along with very compact programs. However, even Tiny OSs are subject to the same follies as their larger counterparts: viruses, injection attacks, buffer overflows, and the like. Further, programs are error-prone and changeable, and thus are also open to attacks.

2.3. Bionanotechnology

Combining living organisms from biotechnology with mechanical intelligence from nanotechnology has also given rise to whole new areas of science. Applying combined bionanotechnology requires, on the bio-side, knowledge of proteins, amino acids, nucleic acid, and cell adsorption on surfaces. Bio-knowledge is coupled with nano-knowledge that includes physics, chemistry, and engineering as applied to nano capabilities, methods, and contexts. The technology-knowledge includes computing, quantum interface management, tiny operating systems, and so on. In short, it is as Arthur C Clarke said, "Any suitably advanced technology is indistinguishable from magic" (Clarke on brainyquotes.com, 1961). With applications from space to health to robotics, the only limits on our use of bionanotechnology are the imaginations of its creators.

3. Benefits from Emerging Technologies

This section describes the benefits of biotechnology, nanotechnology, and bionanotechnology.

3.1. Biotechnology

Biotechnology provides better, faster, cheaper, and less-invasive health management plus targeted medicine delivery, extended product shelf-lives, reduced pollution, reduced energy use,

improved product quality, and, for foods, minimal growth of bacteria, yeast, or mold. The arguments for biotechnology are compelling. Even with resistance, which has lessened as economic conditions have deteriorated, bioengineered products are finding their way into everyday life.

Some notable milestones for bio-engineered crops are the beginning of seven million acres of biotech commodity crops in 1996 and the rapid adoption rate to the present. In 2005, the one-billionth acre of biologically engineered crops was planted in the northern hemisphere. As of 2007, the number of countries growing bio-engineered crops went from five in 1996 to 23 with the top ten countries in terms of acreage including: USA, Argentina, Brazil, Canada, India, China, Paraguay, South Africa, Uruguay, Philippines. And, "2007 marked the first year when the accumulated number of farmer decisions to adopt biotech crops has exceeded 50 million" (ISAAA,org, 2008).

Crop/food engineering has become a well-understood science with a standard protocol not just for the science but also for the introduction of the crops into new countries (Gregory et al, 2008). Plus, bioengineered food crops are big business – "the global value of the biotech crop market is projected at approximately US $7.5 billion for 2008" (Cropnosis as cited by ISAAA.Org, 2008). As of 2008, all major crops – wheat, rice, maize, soybeans cotton and canola – have undergone substantial bio-engineering to improve resistance to disease, shelf-life, speed of growth, and amount of yield (Gregory et al, 2008). In addition, large-scale projects to improve the genetics of eggplant, papaya, tomato, banana, cabbage and cauliflower are underway (Gregory et al, 2008). Thus, even with complexities of bio-technology development, stunning changes impact our daily lives.

3.2. Nanotechnology

Nanotechnology miniaturizes products such that minimal raw materials are used. Resulting nano-scale products have desirable economic qualities such as reduced cost, increased automation, and increased imbedded intelligence in device operation.

The approximately 50 micron transmission at right shows "part of a system capable of increasing the force out of a microengine by a factor of 3,000,000" (Memxorg, 2008). Memristors, a form of nano-scale resistor, has unique properties that will allow it to extend Moore's Law beyond current physical limitations: "Variable resistance and the ability to remember the resistance even when the power is off" (Greene, 2008, p 1). Ultimately, memristors will provide greater performance at lower energy.

Monitoring of all types becomes economically feasible. At present, micron-sized nano-devices are used in building environmental control systems to automatically turn on and off lights based on heat-signature presence, adjust heating and cooling to the heat-signature presence in a room, provide remote home environment or light management, and so on. Some governments are experimenting with these devices to save lives by knowing, in advance, the enemy's combat strength.

Because of carbon nano tubes unique properties – conductivity, tensile and intrinsic strength, when added to traditional polymers, they result in novel materials with expanded applications. One example is to have nano-scale antimicrobial agents imbedded in food packaging to enhance shelf life. They can also increase or decrease gas permeability for applications requiring gas transfer.

Nano-particles are being used in sunscreens to ensure total coverage; in clothing to increase life of the object and be self-cleaning; in batteries to expand shelf-life and provide faster charge times; and in electronics to make thinner, faster, cheaper, more functional devices (Understandingnano.com, 2008).

4. Bionanotechnology

The combination of bio and nanotechnologies will revolutionize the practice of medicine and dentistry. Biotechnology will eventually identify the means to prolong life into hundreds of years while nanotechnology will deliver the bioengineered products in a manner that will minimize rejection. Some products either being developed or on the horizon include arterial cleaners with nano-injectors, mobile cell repair units, dermal displays to integrate computing into human bodies, and robots capable of deciding where, how, and what to mine on asteroids (Foresight.org, 2008).

Further, medicine will be customizable to the patient, cancer cells will be identifiable throughout the body, drugs will be delivered only to 'sick' cells rather than to a whole body, tissue, bone, and tooth growth will all be sped up (Foresight.org, 2008; Understandingnano.com, 2008). Procedures that are currently unpleasant, such as proctology exams or gastro-intestinal exams, will become obsolete as bionanotechnology devices will be ingested and report back on the health of all examined areas. Further, when the devices are done with their original task, they will be able to be shut down or reprogrammed to do other work in the body. This should lead to more timely diagnosis of disease of all types, but should enable faster quarantine of patients who might otherwise spread epidemics (Nanotechnologydevelopment.com, 2008).

Other applications of bionanotechnology relate to environmental improvement. Garbage dumps, waste treatment, forest fires, and pollution should be eradicable by use of bionano devices to 'eat' the offending materials, reducing them to their elements.

Computing support for intelligent bionano devices is under development by IBM, Intel, ST Micro and others. A consortium of these companies recently was credited with building the "world's smallest static random access memory (SRAM)" and the group is at work on a 32 nm gate array for a 22 nm technology node (Nanotechnologydevelopment.com, 2008). The first TinyOS® was created at Berkeley as part of the smart mote project as long ago as 1999 and has become the industry de facto standard (Tinyos.net, 2008).

5.Threats from Emerging Technologies

Threats from biotechnologies and nanotechnologies are present in every area of research. The problem is that most research focuses only on commercializing results and not also on mitigating any inherent risks. As a result, the risks become critical as humans are incapable of detecting,

protecting against, or fixing any problems that arise from bionanotechnologies. This section briefly describes the more critical health and computing threats posed by bionanotechnologies.

5.1. Infrastructure threats

TinyOS, like Windows and active RFID OSs, is subject to viruses, worms, and hacks that exploit buffer overflows. An example is that a person buys a piece of smart luggage with a built-in a chemical security sensor so the individual can move through an airport faster. Unknown to the owner, the sensor has been hacked and told to infect all nearby wireless devices with a virus. Since all luggage will have similar sensors, they will rapidly become infected, as does the airport network, the airline networks, and so on. Instead of taking hours to move around the globe, nanotechnology will allow a virus attack to move within minutes to shut down global communications and computing. Eugene Kaspersky, a recognized expert in viruses and other forms of computer attacks, has said that the number of virus attacks is over 20 per minute. Most, because they are computer generated, are based on a known virus signature. As virus hackers become more knowledgeable, possibly using nanotechnology themselves, viruses will become more novel and take longer to identify (kaspersky.com, 2008). As a result of these compound problems, mitigating virus, worm, and buffer overflow attacks before TinyOS is ubiquitous is critical to global computing safety.

5.2. Monitoring

Smart motes, commercialized as Smart Dust and first developed at Berkeley in the late 1990s, has undergone four radically different generations of development. The first generation was a 2-inch by 2-inch device that has been commercialized for building environmental controls. The present generation shown in the photo at right is now a two nanometer device capable of changing shape so that when deployed from an airplane, it can either drop to the ground or be carried on wind currents. Smart Dust imbeds the TinyOS plus wireless communications, coming to life only every 15-20 minutes to preserve the battery and provide two to three years of active life. Smart motes form self-organizing networks with the nodes doing some sort of sensing and the server reporting the sensor readings. Since communications are two-way, smart dust is able to be repurposed. The sensors shown in the photo are meant to be airborne but other species of them are meant to be aerosoled, painted, ingested, or imbedded in other devices, such as upholstery, clothing, or carpeting.

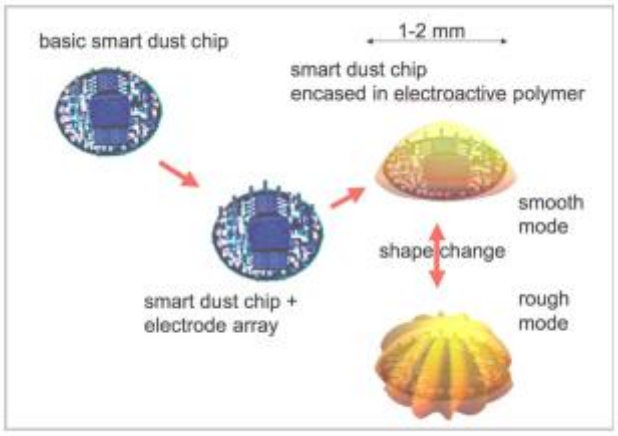

Figure 3. 2nm Smart Dust

These devices can provide monitoring on every human on earth. While some might think this is an acceptable trade-off for eliminating, or managing, terrorism, the massive loss of personal privacy deserves some public discussion.

In another scenario, smart motes can be used for industrial espionage. Since there is currently no known human way to determine the presence of nano-sized devices, other nano-sized devices will be required to provide friendly surveillance. In this scenario, the friendlies will be monitoring for enemy devices and either will neutralize them, or destroy them, or be taken over by them ( ). The point of this discussion is that, without the means of detecting the presence of nano-sized devices, espionage will be taken to new levels.

5.3. Health Risks

Some known health risks from smart mote-type devices are already identified. There are risks from electromagnetic energy that, so far, have gone unresearched (Albrecht & McIntyre, 2004; Singer, 2003). Carbon nanotubes, the basis for most bionanotechnology have been found to cause reactions in protozoa such that the cells eventually die (Wilson, 2008). Further, since 2003, the permeation of 100nm or smaller particles by human skin has been known and warned about as a threat to humanity that has been largely ignored (SmallTimes.com, 2003).

Once broadly deployed, nano-scale devices pose unknown risks to human existence. Mature mote technology will be able to manipulate life forms (Singer, 2003; Pelesko, 2005; Warnecke, et al., 2001). In one scenario, every device is given a task to change cell structure or purpose in a unique way in human bodies. Because so many variations of cellular attack will be taking place, the likelihood of timely diagnosis and treatment is reduced. Attacks could be randomly mounted so identifying the source becomes impossible. Massive loss of life would be expected.

When considering the computing risks, today, humans have dumb, i.e., non-intelligent, non-reprogrammable, non-communicating, devices such as pacemakers and insulin pumps installed to manage health problems. Once these devices become intelligent, issues such as hardening and firewalls become imperative. Hardening is the turning off of unwanted features and functions performed in a data center by security and operating system specialists. Carried into the bionanotechnology realm, hardening will be customized to the patient and conducted by doctors and computing specialists. Devices will require extensive pre-insertion testing to guarantee them free of viruses and so on. Once deployed, smart bionanotechnology will not easily be removed. Further, there is currently no means to detect or stop unwanted bionanotechnology agents from operating in a body. Yet, foods, drinks, and medicines are expected to contain nanotechnology for improved product characteristics. Therefore, some pre-deployment design to prevent device hacking is imperative.

5.4. Environmental Risks

The risks above that relate to health carry over to environmental risks. Consider the risk from repurposeable motes in a nuclear facility. The motes could first neutralize the staff, then alter the functioning of the facility with a negative outcome. Similarly, the same type of attack on the water supplies of large cities could easily wipe out most of humankind. Another similar potential is for nano-scale sensors tasked with seismic monitoring to be retasked to cause earthquakes (SmallTimes.com, 2003). There is no half-life of self-replicating organisms and, since risks were made known in 2003, no prevention of these potentials has taken place (Bennet, et al., 2005).

6. Proposed Changes in Emerging Technology Development

Alternatives for action include doing nothing, laissez-faire, creation of a security state with militant paternalism, social transparency, mutual accountability in a reciprocal environment (Wood, 2007). The first two alternatives beg the dire consequences identified above and, therefore, are unacceptable. The security state, while feasible, seems not the ideal alternative because in world history security states tend to become repressive dictatorships. Therefore, social transparency and mutual accountability become the real alternatives. These alternatives are not mutually exclusive and, mutual accountability may only be possible with full transparency. Therefore, these seems to be the desired social end-states.

None of the above alternatives give or assume any direction for governments to take. If the OECD's 1980 privacy guidelines were taken as a direction, something similar could be developed for bionanotechnologies. This adaptation would include directives on, for instance, deployment, life cycle, communication, security, usage, purpose, openness, and accountability. While such guidelines are useful for organizations that participate in society, they are useless in regulating renegades. Thus, while desirable, government directives, whether local or global, are unlikely to actually regulate much activity.

Technical solutions should also be considered. First, risk analysis on each application of each technology could be performed and the risks mitigated as products are developed. Authentication for change authorization and code access are critical to preventing casual hacks. Signals to and from devices should be required to be encrypted. Some method of disabling nanodevices and/or their self-replicating mechanisms should be imbedded in every device (cf. Konidala, et al, 2006). A 'privacy bit' could be imbedded in each nanodevice to allow only legitimate readers information access (cf. OECD, 2006; Konidala, et al, 2006). Perhaps clothing could include fail-safe mechanisms that would shutdown all nanodevices within, for example, a 2-foot radius. Finally, technology design could be forced to include failsafe mechanisms that can be override all other programming, as needed (cf. Konidala, et al., 2006).

The problem with all of these solutions is that they all appear to be temporary. As intelligent, self-replicating devices proliferate, the risks to human viability become clear. Government regulation, mutual accountability with full transparency, and failsafe mechanisms for all nano-scale devices all will be required to provide a minimum of safety in their use. Beyond these measures, teaching of social responsibility will be needed to enlist a global army to vigilance against anyone violating the norms.

7. Conclusions

While bio technologies and nanotechnologies offer the promise of improving many aspects of life, no technology is free of negative consequences. If antidotes and safeguards to mitigate risks are not built into any bionano initiatives, the consequences could be disastrous.

References on Request.